(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Patentschrift**

(10) **DE 28 11 872 C 1**

(51) Int. Cl.[5]: **H 04 K 1/00**

(21) Aktenzeichen: P 28 11 872.1-35
(22) Anmeldetag: 18. 3. 78
(43) Offenlegungstag: –
(45) Veröffentlichungstag der Patenterteilung: 7. 1. 93

Erteilt nach § 54 PatG in der ab 1. 1. 81 geltenden Fassung
Innerhalb von 3 Monaten nach Veröffentlichung der Erteilung kann Einspruch erhoben werden

(73) Patentinhaber:
ANT Nachrichtentechnik GmbH, 7150 Backnang, DE

(72) Erfinder:
Bitzer, Wolfgang, Dipl.-Ing., 7153 Weissach, DE

(56) Für die Beurteilung der Patentfähigkeit in Betracht gezogene Druckschriften:
AFJPS-Conference Proceedings, Vol. 45, S.109-112;

(54) Verfahren zur Schlüsselzuteilung

DE 28 11 872 C1

DE 28 11 872 C1

Beschreibung

Die Erfindung betrifft ein Verfahren zur geheimen Vereinbarung eines gemeinsamen Grundschlüssels zwischen zwei mit elektronischen Schlüsselgeräten ausgestatteten Sende-Empfangsstationen A und B, die durch eine elektrische Nachrichtenverbindung duplex- oder halbduplex miteinander verbunden sind und zuvor über keine gemeinsame Geheimschlüsselinformation verfügen müssen.

Aufgabe der Erfindung ist es, hierbei eine gemeinsame Schlüsselinformation zuzuteilen, ohne daß ein Dritter (Unbefugter) sich diesen Schlüssel in endlicher Zeit ableiten kann.

Dabei ist es nicht erforderlich, daß noch eine dritte Stelle an dieser Prozedur mitwirkt oder daß die beiden Teilnehmer von vornherein über eine Schlüsselinformation verfügen.

Wenn Nachrichten verschlüsselt von einer Stelle zu einer anderen übertragen werden sollen, so ist eine unabdingbare Voraussetzung, daß diese beiden Stellen über dieselbe Schlüsselinformation verfügen. Diese Schlüsselinformation kann elektrisch oder elektromechanisch in den Geräten gespeichert sein, oder sie kann z. B. bei Bedarf von einer Bedienungsperson eingegeben werden. Auf jeden Fall muß sie aber in irgendeiner Form bei den Teilnehmern der verschlüsselten Übertragung vorhanden sein, was immer — insbesondere bei umfangreicheren Netzen — die Gefahr einer Kompromittierung des Schlüsselmaterials mit sich bringt.

In den amerikanischen Verschlüsselungssystemen "Vinson" und "Tenley" werden Verfahren verwendet, bei welchen den Teilnehmern einer verschlüsselten Übertragung zuvor das benötigte Schlüsselmaterial von einer Schlüsselzentrale aus zugeteilt wird. Hierzu ist aber erforderlich, daß diese Teilnehmer über persönliche Schlüssel verfügen, mit denen das benötigte Schlüsselmaterial verschlüsselt von der Schlüsselzentrale zu diesen übertragen wird. Diese persönlichen Schlüssel müssen außer bei den jeweiligen Teilnehmern auch noch in den Schlüsselzentralen abgespeichert sein, was auch wieder nachteilig ist:

- Die persönlichen Schlüssel können kompromittiert werden.
- Die Schlüsselzentrale kann ausfallen.
- Die persönlichen Schlüssel müssen zuvor zugeteilt werden, was einen relativ großen Verwaltungsaufwand bedeutet und manchmal auch gar nicht möglich ist.

Ein Verfahren, das ohne persönliche Schlüssel und ohne Schlüsselzentrale über große Entfernungen eine elektronische Schlüsselzuteilung gestattet und dabei sicher verhindert, daß sich ein Unbefugter in den Besitz dieses Schlüssels setzt, ist bisher nicht bekannt.

In "Multiuser cryptographic techniques" von Diffie und Hellmann, AFIPS-Conference proceedings, Vol. 45, Seiten 109 bis 112, ist auf Seite 110, rechte Spalte, unter der Überschrift "Public Key Cryptography" die Aufgabenstellung für ein System beschrieben, das ebenfalls die gestellte Aufgabe, auf eine physikalische Schlüsselverteilung verzichten zu können, lösen soll. Es beruht auf der gedanklichen Voraussetzung, daß es jeweils zwei korrespondierende Schlüssel E und D gebe, von denen eine (E) nur zur Verschlüsselung und der andere (D) nur zur Entschlüsselung verwendet werden soll. Für den Uneingeweihten soll sich D aus E nicht berechnen lassen. Deshalb soll E veröffentlicht werden können, und nur der Besitzer des (geheimzuhaltenden) Schlüssels D soll die damit verschlüsselte Nachricht entschlüsseln können. Es wird aber in derselben Fundstelle (Seite 111, 1. Absatz) beschrieben, daß die gestellte Aufgabe bisher nicht gelöst sei.

Nachteilig wäre bei diesem Verfahren außerdem, daß für alle Teilnehmer die zur Entschlüsselung erforderlichen Schlüssel D individuell berechnet und geheim abgespeichert werden müssen.

Das nachfolgend beschriebene Verfahren soll demgegenüber ermöglichen, daß zwei duplex- oder halbduplex (z. B. über Funk) miteinander verbundene Stationen denselben Grundschlüssel erhalten, ohne daß hierzu eine dritte Stelle (Schlüsselzentrale) eingeschaltet werden muß, ohne daß schon vorher Schlüsselmaterial (persönliche Schlüssel o. ä.) vorhanden sein muß und ohne daß ein Unbefugter, auch wenn er den Übertragungsweg anzapft, diesen Schlüssel erfahren kann.

Gelöst wird die Aufgabe durch die im Hauptanspruch angegebenen Merkmale. Zweckmäßige Weiterbildungen sind in den Unteransprüchen aufgeführt.

Im folgenden soll das erfindungsgemäße Verfahren näher beschrieben werden.

Gegeben sei eine Übertragungsstrecke mit den beiden Endstellen A und B (**Fig.** 1). Diese Übertragungsstrecke kann durch eine Stelle C angezapft werden. Zwischen A und B werden nun Informationen ausgetauscht, aus denen sich A und B den identisch gleichen Schlüssel ausrechnen können, wozu aber C nicht (oder jedenfalls nicht in endlicher Zeit) in der Lage sein darf.

Die Stelle A verfügt über eine erste Digitalinformation a und eine zweite x (beide können z. B. Binärzahlen sein). Die Station B verfügt ebenso über eine erste Digitalinformation b und dieselbe Information x wie A. Die Informationen a und b sind geheimzuhalten. Dies ist aber kein Problem, da a nur in A und b nur in B benötigt wird. Die Informationen a und b können z. B. bei Bedarf jedesmal neu durch z. B. einen echten Zufallszahlengenerator (Rauschgenerator) erzeugt werden.

Die Information x muß sowohl in A als auch in B identisch gleich sein. Sie kann hier fest eingespeichert sein, aus Datum-Uhrzeit abgeleitet werden oder auch z. B. von einem Zufallsgenerator erzeugt, von A nach B offen übertragen werden, da sie nicht geheimgehalten werden muß. Der Anzapfer C darf sie erfahren.

Die Prozedur läuft nun folgendermaßen ab (**Fig.** 2):

a) Stelle A bildet eine Verknüpfung von einer ersten Information a mit einer zweiten Information x. Das Ergebnis dieser Verknüpfung f (a, x) — beispielsweise eine Binärzahl — wird offen (nicht geheimgehalten) zu B übertragen (es kann auch verschlüsselt übertragen werden).

b) Stelle B wendet auf diesen übertragenen Wert f (a, x) nochmals dieselbe Verknüpfung — diesmal aber

mit einer dritten Information b — an, bildet also f (b, f (a, x)), was wieder eine Binärzahl sein kann, die als geheime Schlüsselinformation an das Schlüsselgerät weitergegeben wird.
c) Stelle B berechnet f (b, x), was wieder (offen) zu A übertragen wird.
d) Stelle A wendet hierauf wieder dieselbe Verknüpfungsvorschrift mit der Größe a an, berechnet also f (a, f (b, x)). Dieser Wert wird auch hier als geheime Schlüsselinformation an das Schlüsselgerät gegeben.
Denkbar sind auch Verknüpfungsvorschriften f (y, x, x_0). Die beiden Werte x, x_0 spielen hier die gleiche Rolle wie vorher x, d. h. sie müssen an beiden Stellen A und B gleichermaßen bekannt sein. Speziell kann z. B. auch $x = x_0$ oder $x_0 = 0$ oder $x_0 = 1$ gesetzt werden. Die Prozedur läuft dann genau so ab, wie oben beschrieben, es wird jetzt aber gebildet:

in Stufe a)	f (a, x, x_0)
in Stufe b)	f (b, x, f (a, x, x_0))
in Stufe c)	f (b, x, x_0)
in Stufe d)	f (a, x, f (b, x, x_0))

Die im folgenden angegebenen Forderungen an die Verknüpfungsvorschriften f gelten dann hierfür sinngemäß genauso.

Im Vorhergehenden ist unter der Funktion f (y, x) immer dieselbe Verknüpfungsvorschrift zu verstehen. Sie muß, damit das Verfahren die gestellte Aufgabe erfüllt, drei Bedingungen erfüllen:

— Beide Stellen A, B müssen natürlich dieselbe geheime Schlüsselinformation erhalten. Es muß also gelten:

f (b, f (a, x)) = f (a, f (b, x))
(Bedingung 1)

Der Abhörer kennt die Informationen x, f (a, x) und f (b, x), nicht aber a und b. Er darf natürlich nicht in der Lage sein, daraus in endlicher Zeit die geheime Schlüsselinformation zu berechnen. Daraus ergibt sich die zweite Bedingung für die Verknüpfungsvorschrift:
— Auch bei Kenntnis von x, f (a, x) und f (b, x) darf es nicht möglich sein, mit endlichem Aufwand in endlicher Zeit daraus a, b oder f (b, f (a, x)) = f (a, f (b, x)) zu berechnen, oder allgemein formuliert:
Bei Kenntnis der Ausgangsgröße f (y, x) und einer Eingangsgröße x, darf es nicht möglich sein, mit endlichem Aufwand in endlicher Zeit daraus die andere Eingangsgröße y zu berechnen. (Bedingung 2)
Schließlich nützt es nichts, wenn auch die Stellen A und B einen ins unermeßliche gehenden Aufwand treiben müssen, um die Funktion f (y, x) zu berechnen. Daraus resultiert die dritte Bedingung:
— Bei Kenntnis der beiden eingangsseitigen Größen y, x muß die Ausgangsgröße b (y, x) mit geringem Aufwand in kurzer Zeit berechenbar sein. (Bedingung 3)

Verknüpfungsvorschriften, die die im vorangegangenen Abschnitt aufgestellten Forderungen erfüllen, sind beispielsweise die Multiplikation und die Exponentiation modulo p, also im Galoisfeld (GF) p, wobei p eine Primzahl sein sollte. Die Addition modulo p erfüllt die Bedingung 2 nicht, während diese von der Exponentiation am besten erfüllt wird.
Diese Funktionen sind in der Tabelle der **Fig.** 3 zusammengestellt.
Die Verknüpfungsvorschrift der Form f (y, x, x_0) kann realisiert werden durch die y-mal wiederholte Anwendung einer Verknüpfung F (x, z) in der Form:

$$f(y, x, x_0) = \underbrace{F(x, F(x, F(x, \ldots F(x, x_0) \ldots)))}_{y \text{ mal}}$$

Diese Formel ist eine allgemeine Vorschrift zur Konstruktion von in Frage kommenden Verknüpfungen f (y, x) bzw. f (y, x, x_0).
Für F (x, z) läßt sich eine ganz beliebige Funktion (beliebig nichtlinear) verwenden. Beispielsweise könnte F (x, z) ein Schlüsselvorgang sein mit z als Eingangsgröße und x als Schlüssel.
Die angeführten Berechnungen werden zweckmäßigerweise mittels Binärzahlen durchgeführt. Als Primzahl p wird eine Primzahl der Form

$$p = 2^{2n} - 1$$

oder

$$p = 2^{2n} + 1$$

empfohlen.
Die Rechnung modulo p erfolgt dann einfach durch Abschneiden des Überlaufs und Addieren desselben zu bzw. Abziehen desselben von der verbleibenden Binärzahl. Die Berechnung der Potenzen x^y erfolgt durch

fortlaufende Multiplikation von Zweierpotenzen von x modulo p:

$$x^y \text{ modulo } p = x^{(a_0 \cdot 2^0 + a_1 \cdot 2^1 + a_2 \cdot 2^2 +)} \ldots \text{mod. } p$$

$$= x^{a_0 \cdot 2^0} \cdot x^{a_1 2^1} \ldots \text{mod. } p$$

mit
$a_\nu \in \{0,1\}$

$\nu = 1, 2, 3 \ldots$

während die Multiplikationen als Summierung von Zweierpotenzen ausgeführt werden:

$$x \cdot y \text{ modulo } p =$$

$$\sum_{\nu=0}^{n} a_\nu \cdot 2^\nu \cdot x \text{ modulo } p$$

wieder mit $a_\nu \in \{0,1\}$

Fig. 4 zeigt ein Beispiel für eine Anordnung zur Durchführung des Verfahrens. Anhand dieser Figur soll der Ablauf der Prozedur nochmals im Zusammenhang erläutert werden.

Die beiden Stationen **1, 2** eines Nachrichtennetzes sind über die nicht näher dargestellte Übertragungsstrecke **3** miteinander verbunden. Sie enthalten je ein Schlüsselgerät **4, 5** zur Ver- bzw. Entschlüsselung der zu übertragenden Information. Der Schlüssel dieser Schlüsselgeräte **4, 5** wird in je einem zugeordneten Schlüsselspeicher **6, 7** abgespeichert.

Angenommen, die erste Station **1** will nun mit der zweiten Station **2** einen gemeinsamen Schlüssel vereinbaren, der in den Schlüsselspeichern **6, 7** abgelegt werden soll.

Hierzu wird zunächst die in einem ersten Speicher **10** gespeicherte Information a mit der in einem zweiten Speicher **12** gespeicherten Größe x in der Verknüpfungsschaltung **8** verknüpft. Das Ergebnis dieser Verknüpfung, f (a, x), gelangt über den Umschalter **15**, die Übertragungsstrecke **3** zur Station **2**, wo es über den Umschalter **16** zu der mit **8** identisch gleichen Verknüpfungsschaltung **9** gelangt, wo es mit der in dem ersten Speicher **11** abgespeicherten Information b zu dem Ergebnis f (b, f (a, x)) verknüpft wird, das dann über den Umschalter **17** dem Schlüsselspeicher **7** zugeführt wird.

Zur Durchführung der Prozedur in der Gegenrichtung werden die Umschalter **14, 15, 16** und **17** in die andere Lage gebracht. Die im zweiten Speicher **13** gespeicherte Größe x wird über den Umschalter **16** der Verknüpfungsschaltung **9** zugeführt, wo sie mit der im ersten Speicher **11** abgespeicherten Information b zu f (b, x) verknüpft wird.

Dieser Wert wird dann über den Umschalter **17**, die Übertragungsstrecke **3** und den Umschalter **14** zur Verknüpfungsschaltung **8** übertragen, wo er mit der im ersten Speicher **10** abgespeicherten Information a in der Verknüpfungsschaltung **8** zu f (a, f (b, x)) verknüpft wird. Dieses Ergebnis wird dann über den Umschalter **15** in den Schlüsselspeicher **6** abgelegt.

Somit verfügen jetzt beide Schlüsselgeräte **4, 5** in den ihnen zugeordneten Schlüsselspeichern **6, 7** über den identisch gleichen Schlüssel und die verschlüsselte Übertragung der Nutzinformation über die Klartext-Klemmenpaare **22, 23** der Schlüsselgeräte kann beginnen.

Für die Umschalter **14, 15, 16** und **17** werden zweckmäßigerweise automatisch gesteuerte elektronische Schalter (Torschaltungen) eingesetzt.

Die Informationen a können in vorteilhafter Weise durch Zufallsfolgengeneratoren **18, 19** erzeugt und von dort den Speichern **10, 11** zugeführt werden.

Diese Zufallsfolgengeneratoren **18, 19** können auch dazu verwendet werden, in einer Station (z. B. **1**) die Größe x in zufälliger Weise zu erzeugen, die dann dem Speicher (z. B. **12**) zugeführt und gleichzeitig über die Übertragungsstrecke **3** übertragen, dem Speicher (z. B. **13**) der Gegenstation (z. B. **2**) zugeführt wird.

Die Größe x kann aber auch in den Speichern **12, 13** einmalig (evtl. geheim) fest eingestellt sein oder sie kann z. B. durch in beiden Stationen gleiche Uhrenschaltungen **20, 21** zu jeder Zeit in beiden Stationen identisch den Speichern **12, 13** zur Verfügung gestellt werden.

Die dargestellten Schaltungen können mit kommerziell erhältlichen digitalen Schaltkreisen aufgebaut werden, zur Realisierung der Verknüpfungsschaltung **8, 9** sowie der (nicht in der Zeichnung dargestellten) Steuerung für den gesamten Prozedurablauf können mit Vorteil Mikroprozessorschaltungen eingesetzt werden.

Patentansprüche

1. Verfahren zur geheimen Vereinbarung eines gemeinsamen Grundschlüssels zwischen zwei mit elektronischen Schlüsselgeräten ausgestatteten Sende-Empfangsstationen A und B, die durch eine elektrische Nachrichtenverbindung duplex- oder halbduplex miteinander verbunden sind und zuvor über keine gemeinsame Geheimschlüsselinformation verfügen müssen, **dadurch gekennzeichnet**, daß die erste Station (A) über eine erste Information (a) und eine zweite Information (x) verfügt, daß die zweite Station (B) über die gleiche zweite Information (x) und eine dritte Information (b) verfügt, daß die erste und dritte Information (a, b) geheimgehalten wird, während die gemeinsame zweite Information (x) offen sein kann, daß die erste

Station (A) eine erste Verknüpfung f (a, x) bildet, deren Ergebnis zur zweiten Station (B) übertragen wird, daß die zweite Station (B) nach der gleichen Verknüpfungsvorschrift eine zweite Verknüpfung f (b, x) bildet, deren Ergebnis zur ersten Station (A) übertragen wird, daß die zweite Station (B) aus dem ihr übertragenen Wert der ersten Verknüpfung f (a, x) mittels derselben Verknüpfung mit der dritten Information (b) die Größe f (b, f (a, x)) und die erste Station (A) aus dem übertragenen Wert der ersten Größe f (b, x) durch dieselbe Verknüpfung mit der ersten Information (a) die Größe f (a, f (b, x) bildet, daß die Verknüpfungsvorschrift f (y, x) derart gewählt ist, daß gilt:

$$f(b, f(a, x)) = f(a, f(b, x))$$

und daß diese Größe bei der ersten und zweiten Station (A, B) als Geheimschlüsselinformation verwendet wird.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß die Verknüpfungsvorschrift f (y, x) außerdem so gewählt ist, daß bei Kenntnis der Eingangsgröße (y) und der zweiten Information (x) die Größe f (y, x) mit geringem Aufwand in kurzer Zeit berechenbar ist, daß aber bei Kenntnis der Verknüpfungsvorschrift f (y, x) sowie der zweiten Information (x) die Eingangsgröße (y) nur mit sehr großem Aufwand in sehr langer Zeit berechenbar ist.

3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß die zweite Information (x) in allen Geräten fest abgespeichert ist.

4. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß die zweite Information (x) aus einer überall bekannten Information, beispielsweise Datum oder Uhrzeit, abgeleitet ist.

5. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß die zweite Information (x) in einer der beiden Stationen (A oder B) durch einen elektronischen Zufallszeichengenerator erzeugt und zur anderen Station übertragen wird.

6. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß die Informationen, Werte und Größen in der Form von Binärzahlen dargestellt sind und die notwendigen Verknüpfungen als Rechnungen mit Binärzahlen durchgeführt werden.

7. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß folgende Verknüpfungsvorschrift verwendet wird:

$$f(a, x) = a \cdot x \text{ modulo } p$$
$$f(b, x) = b \cdot x \text{ modulo } p$$
$$f(b(f(a, x)) = b \cdot a \cdot x \text{ modulo } p$$
$$= a \cdot b \cdot x \text{ modulo } p = f(a(f(b, x))$$

8. Verfahren nach einem oder mehreren der Ansprüche 1 bis 6, dadurch gekennzeichnet, daß folgende Verknüpfungsvorschrift verwendet wird:

$$f(a, x) = x^a \text{ modulo } p$$
$$f(b, x) = x^b \text{ modulo } p$$
$$f(b, f(a, x)) = (x^a)^b \text{ modulo } p = x^{ab} \text{ modulo } p =$$
$$x^{ba} \text{ modulo } p = (x^b)^a \text{ modulo } p = f(a, f(b, x))$$

9. Verfahren nach Anspruch 7 oder 8, dadurch gekennzeichnet, daß p eine Primärzahl ist.

10. Verfahren nach Anspruch 9, dadurch gekennzeichnet, daß für p eine Primzahl der Form

$$p = 2^{2^n} - 1 \text{ oder } 2^{2^n} + 1$$

verwendet ist, wobei n eine ganze positive Zahl ist.

11. Verfahren nach einem oder mehreren der vorangehenden Ansprüche, dadurch gekennzeichnet, daß die erste Information (a) und/oder die dritte Information (b) in den Stellen (A bzw. B) vor jeder Durchführung des Verfahrens durch je einen Zufallsgenerator an Ort und Stelle neu erzeugt und abgespeichert wird und nicht aus den Geräten ausgebbar ist.

12. Verfahren nach einem oder mehreren der vorangegangenen Ansprüche, dadurch gekennzeichnet, daß die erzeugte Schlüsselinformation f (b, f (a, x)) = f (a, f (b, x) in den Schlüsselgeräten der Stellen (B bzw. A) zusätzlich zu einem dort bereits abgespeicherten geheimen Grundschlüssel verwendet wird.

13. Anordnung zur Durchführung des Verfahrens nach einem der vorhergehenden Ansprüche mit mindestens zwei Stationen, die durch eine elektrische Übertragungsstrecke miteinander verbunden sind, die je ein Schlüsselgerät zur Verschlüsselung von Daten oder Sprachsignalen enthalten, denen der hierzu erforderliche Schlüssel aus einem elektronischen Schlüsselspeicher zugeführt wird, dadurch gekennzeichnet, daß dieser Schlüssel diesem Schlüsselspeicher (6, 7) aus einer Verknüpfungsschaltung (8, 9) zugeführt wird, die ihn durch eine mathematische Verknüpfung einer lokal in einem ersten elektronischen Speicher (10, 11) gespeicherten Information (a, b) mit einer von der Gegenstelle über die Übertragungsstrecke (3) übertragenen Größe erzeugt, daß diese Größe dort zuvor mittels derselben Verknüpfungsschaltung (8, 9) durch Verknüpfung einer in beiden Stationen (2, 1) identisch gleich in einem zweiten elektronischen Speicher (12, 13) abgespeicherten zweiten Information (x) mit derselben in dem ersten elektronischen Speicher (10, 11) lokal abgespeicherten Information (a, b) erzeugt wurde und daß die Verknüpfungsschaltung (8, 9) den in einem oder mehreren der vorhergehenden Ansprüche aufgestellten Bedingungen genügt.

14. Anordnung nach Anspruch 13, dadurch gekennzeichnet, daß der erste elektronische Speicher (**10, 11**) für die Information a bzw. b von einem Zufallsgenerator (**18, 19**) geladen wird, der die Information a bzw. b in zufälliger oder quasizufälliger Weise erzeugt.

15. Anordnung nach Anspruch 13 oder 14, dadurch gekennzeichnet, daß die den beiden Stationen (**1**) und (**2**) gemeinsame Größe, die zweite Information (x) dem zweiten elektronischen Speicher (**12, 13**) von je einer elektronischen Uhrenschaltung (**20, 21**) zugeführt wird, die in bekannter Weise so aufgebaut ist, daß sie zur selben Zeit in allen Stationen (**1, 2**) denselben Wert liefert.

16. Anordnung nach Anspruch 13 oder 14, dadurch gekennzeichnet, daß die den beiden Stationen (**1, 2**) gemeinsame Größe (x) durch einen Zufallsfolgengenerator, der mit dem vorhin erwähnten Zufallsfolgengenerator (**18**) identisch sein kann in einer der beiden Stationen (**1**) erzeugt, dort in dem zweiten elektronischen Speicher (**12**) gespeichert, über den elektrischen Übertragungsweg (**3**) zur Gegenstation (**2**) übertragen und dort ebenfalls in dem zweiten elektronischen Speicher (**13**) gespeichert wird.

Hierzu 3 Seite(n) Zeichnungen

– Leerseite –

Nummer: DE 28 11 872 C1
Int. Cl.[5]: H 04 K 1/00
Veröffentlichungstag: 7. Januar 1993

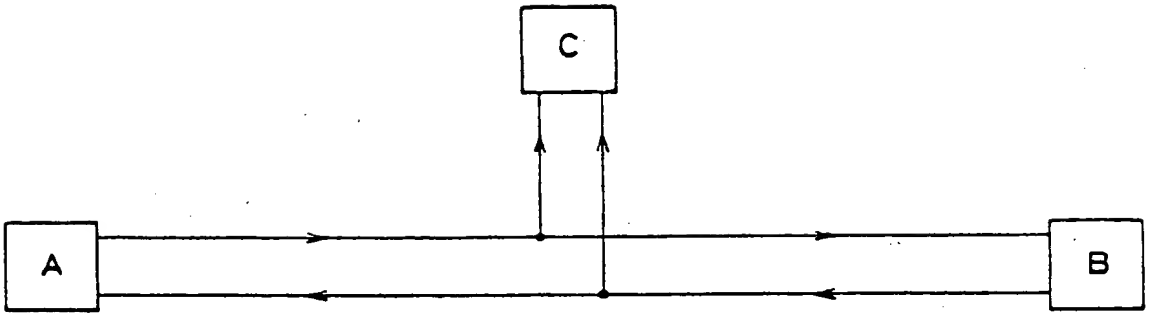
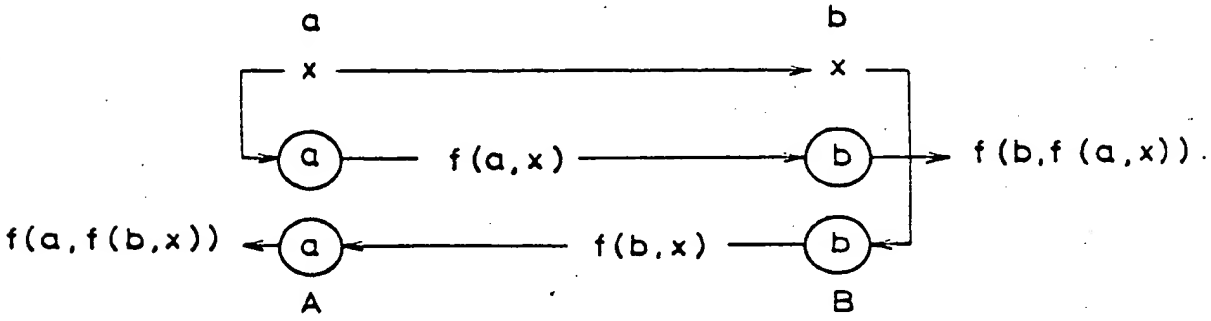


Fig. 1



$$f(a,f(b,x)) = f(b,f(a,x))$$

gemeinsame, geheime Schlüsselinformationen

Fig. 2

Nr.	Verknüpfung	f (y, x)	f (a, x)	f (b, x)	f (b, f (a, x))	f (a, f (b, x))	erfüllt Bed. x) 1	2	3
1	Addition	y + x mod p	a + x mod p	b + x mod p	b + a + x mod p	a + b + x mod p	x	-	(x)
2	Multiplik.	yx mod p	ax mod p	bx mod p	bax mod p	abx mod p	x	x	x
3	Exponent.	x^y mod p	x^a mod p	x^b mod p	x^b mod p	x^{ba} mod p	x	(x)	x
4	Mehrf.Expon.	$x^{x^{\cdot^{\cdot^{x}}}}$ mod p (y mal)	$x^{x^{\cdot^{\cdot^{x}}}}$ mod p (a mal)	$x^{x^{\cdot^{\cdot^{x}}}}$ mod p (b mal)	$x^{x^{\cdot^{\cdot^{x}}}}$ mod p (a + b mal)	$x^{x^{\cdot^{\cdot^{x}}}}$ mod p (b + a mal)	x	(x)	

x) -: nicht erfüllt

x: erfüllt

(x): am besten erfüllt

Mögliche Verknüpfungsvorschriften b (y, x)

Fig. 3

Nummer:
Int. Cl.5:
Veröffentlichungstag: 7. Januar 1993
DE 28 11 872 C1
H 04 K 1/00

Nummer: DE 28 11 872 C1
Int. Cl.[5]: H 04 K 1/00
Veröffentlichungstag: 7. Januar 1993

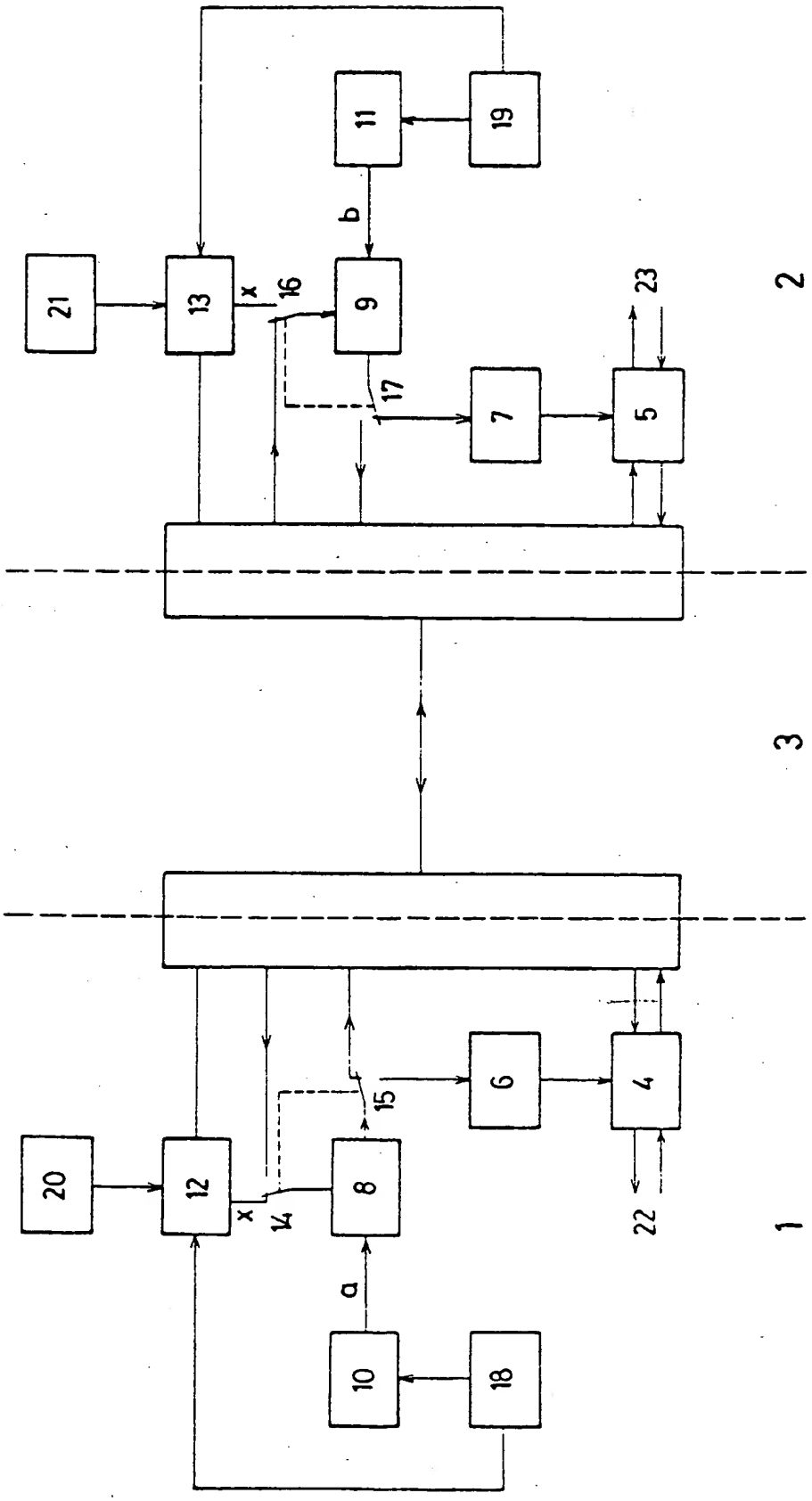


Fig. 4